



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,301	10/09/2001	Philip Hawkes	020002	6013
23696	7590	01/04/2005	EXAMINER	
Qualcomm Incorporated Patents Department 5775 Morehouse Drive San Diego, CA 92121-1714			CERVETTI, DAVID GARCIA	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Applicati n No.

09/973,301

Applicant(s)

HAWKES ET AL.

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 October 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☒ Claim(s) 6 and 7 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 October 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description:

- Figure 1D, reference character 40,
- Figure 2, reference characters 106B, 106H, 106D, 106I, 106F, 106G,
- Figure 5A,
- Figure 7C, reference character 454,
- Figure 7E,
- Figure 8B, reference characters 534, 536,
- Figure 8C, reference characters 534, 538, 550, 552,
- Figure 8D, reference characters 550, 552, 554, and
- Figure 13, reference characters 900, 908, 914.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified

Art Unit: 2136

and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 6 is objected to because of the following informalities: "wherein the short term key identifier is calculated". Perhaps "wherein the short term key is calculated" was intended. Claim 6 has been interpreted as "wherein the short term key is calculated" for the remaining of this document.

Appropriate correction is required.

Claim 7 is objected to because of the following informalities: "ESP". While well known in the art, this term has not been defined.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 21-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 21 states "an infrastructure element for a wireless communication system, comprising: means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; means for determining an access key based on the short term key identifier; means for encrypting the short term key identifier with the access key to recover the short term key; and means for

Art Unit: 2136

decrypting the transmission using the short term key". These limitations are considered non-statutory subject matter because they consist on software code for receiving, determining, encrypting, and decrypting (page 3, paragraph [1007]).

Claim 22 states "a digital signal storage device, comprising: first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; second set of instructions for determining an access key based on the short term key identifier; third set of instructions for encrypting the short term key identifier with the access key to recover the short term key; and fourth set of instructions for decrypting the transmission using the short term key", a digital signal is considered non-statutory subject matter. Furthermore, the limitations are considered non-statutory subject matter because they consist on software code for receiving a short term key identifier, determining an access key based on the short term key identifier, encrypting the short term key identifier with the access key to recover the short term key, and decrypting the transmission using the short term key.

Claim 23 states "a communication signal transmitted on a carrier wave"; a communication signal is considered non-statutory subject matter. Dependent claim 24 is rejected based on its dependency from claim 23.

To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, 14-24 are rejected under 35 U.S.C. 102(b) as being anticipated by
Pierce et al.

Regarding claim 1, Pierce et al. teach a method for secure transmissions, the method comprising: determining a short term key for a message for transmission, the short term key having a short term key identifier (column 2, lines 44-47); determining an access key for the message, the access key having an access key identifier (column 2, lines 47-50); encrypting the message with the access key (column 2, lines 50-52); forming an Internet protocol header comprising the short term key identifier (column 2, lines 52-53); and transmitting the encrypted message with the Internet protocol header (column 2, lines 52-55).

Regarding claim 2, Pierce et al. teach the method as in claim 1, wherein the short term key identifier comprises the access key identifier (column 2, lines 40-58).

Regarding claim 3, Pierce et al. teach the method as in claim 2, wherein short term key identifier further comprises a security parameter index value (column 2, lines 40-58).

Regarding claim 4, Pierce et al. teach the method as in claim 3, wherein the security parameter index value is a random number (column 2, lines 40-58, column 4, lines 55-65).

Regarding claim 5, Pierce et al. teach the method as in claim 1, wherein the short term key is calculated as a function of the short term key identifier and the access key (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 6, Pierce et al. teach the method as in claim 5, wherein the short term key identifier is calculated by encrypting the short term key identifier with the access key (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 14, Pierce et al. teach a method for secure reception of a transmission, the method comprising: receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key (column 4, lines 5-10); determining an access key based on the short term key identifier (column 4, lines 7-13); encrypting the short term key identifier with the access key to recover the short term key (column 4, lines 13-16); and decrypting the transmission using the short term key (column 4, lines 25-30).

Regarding claim 15, Pierce et al. teach the method as in claim 14, further comprising: storing the short term key identifier and short term key in a memory storage unit (figure 1, reference character 111, 105, column 4, lines 5-55).

Regarding claim 16, Pierce et al. teach the method as in claim 14, wherein the short term key identifier is comprised of a random number and an access key identifier associated with the access key (column 4, lines 5-55, column 5, lines 1-25).

Art Unit: 2136

Regarding claim 17, Pierce et al. teach the method as in claim 14, wherein encrypting the short term key identifier further comprises encrypting the short term key identifier and a random number with the access key to recover the short term key (column 4, lines 5-67, column 5, lines 1-25).

Regarding claim 18, Pierce et al. teach in a wireless communication system supporting a broadcast service option (column 3, lines 15-26), an infrastructure element comprising: a receive circuitry (column 4, lines 5-10); a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising: processing unit operative to decrypt key information (column 4, lines 25-30); and a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message, comprising: memory storage unit for storing a plurality of short term keys and short term key identifiers (column 3, lines 26-67, column 4, lines 1-67).

Regarding claim 19, Pierce et al. teach the infrastructure element as in claim 15, wherein the user identification unit further comprises a second memory storage unit for storing a plurality of access keys and access key identifiers (column 4, lines 35-55).

Regarding claim 20, Pierce et al. teach the infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit (column 4, lines 35-55).

Regarding claim 21, Pierce et al. teach an infrastructure element for a wireless communication system (column 3, lines 15-25), comprising: means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; means for determining an access key based on the short term key

Art Unit: 2136

identifier; means for encrypting the short term key identifier with the access key to recover the short term key; and means for decrypting the transmission using the short term key (column 3, lines 53-67, column 4, lines 1-35).

Regarding claim 22, Pierce et al. teach a digital signal storage device, comprising: first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key (column 3, lines 53-67, column 4, lines 1-5); second set of instructions for determining an access key based on the short term key identifier (column 4, lines 5-25); third set of instructions for encrypting the short term key identifier with the access key to recover the short term key (column 4, lines 5-25); and fourth set of instructions for decrypting the transmission using the short term key (column 4, lines 25-35).

Regarding claim 23, Pierce et al. teach a communication signal transmitted on a carrier wave, comprising: a first portion corresponding to a short term key identifier, the short term key identifier having a corresponding short term key; and a second portion corresponding to a transmission payload encrypted using the short term key (column 4, lines 55-67, column 5, lines 1-50).

Regarding claim 24, Pierce et al. teach the communication signal as in claim 23, wherein the short term key identifier comprises: a random number portion; and an access key identifier corresponding to an access key (column 4, lines 55-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pierce et al. as applied to claim 1 above, and further in view of Nessett et al.

Regarding claim 7, Pierce et al. teach the limitations as set forth under claim 1 above. However, Pierce et al. do not disclose expressly the method as in claim 1, wherein the Internet protocol header is part of an ESP header.

Nessett et al. teach the method as in claim 1, wherein the Internet protocol header is part of an ESP header (column 21, lines 53-67).

Pierce et al. and Nessett et al. are analogous art because they are directed to a similar problem solving area – secure network transmission.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Encapsulating Security Payload with the Internet Protocol.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Nessett et al. with the method of Pierce et al. for the benefit of secure network transmissions to obtain the invention as specified in claim 7.

Regarding claim 8, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 7 above. Furthermore, Pierce et al. teach the method as in claim 7, wherein the Internet protocol header further comprises a second random number, the

Art Unit: 2136

second random number having a random number identifier (column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 9, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 8 above. Furthermore, Pierce et al. teach the method as in claim 8, wherein the short term key identifier comprises the access key identifier and the random number identifier (column 2, lines 40-58, column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 10, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 9 above. Furthermore, Pierce et al. teach the method as in claim 9, wherein short term key identifier further comprises a security parameter index value (column 4, lines 35-55).

Regarding claim 11, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 10 above. Furthermore, Pierce et al. teach the method as in claim 10, wherein the security parameter index value is a random number (column 4, lines 35-67, column 5, lines 1-25).

Regarding claim 12, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 8 above. Furthermore, Pierce et al. teach the method as in claim 8, wherein the short term key is calculated as a function of the short term key identifier, the second random number, and the access key (column 4, lines 55-67, column 5, lines 1-25).

Regarding claim 13, Pierce et al. and Nessett et al. teach the limitations as set forth under claim 12 above. Furthermore, Pierce et al. teach the method as in claim 12, wherein the short term key identifier is calculated by encrypting the short term key

Art Unit: 2136

identifier and the second random number with the access key (column 4, lines 5-67,
column 5, lines 1-25).

Art Unit: 2136


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC


EMMANUEL L. NOISE
PRIMARY EXAMINER